PROTEUS SOLUTIONS
IT-Lösungen für den Mittelstand

„Vorratsdatenspeicherung: politische Aussagen und technische Alternativen“

Vorratsdatenspeicherung: politische Aussagen und technische Alternativen

Das Thema Vorratsdatenspeicherung wird schon seit geraumer Zeit in Deutschland diskutiert und ist immer noch politisch ungeklärt. Medien berichten in den verschiedensten Facetten über die Aussagen unserer politischen Führung. Oft werden dabei allerdings nur die entsprechenden Zitate veröffentlicht. Gezielte Aufklärung gegenüber dem Bürger wird allerdings eher vernachlässigt.

Gibt die Vorratsdatenspeicherung unseren Behörden und Gesetzeshütern wirklich effektive Mittel in die Hand im Kampf gegen Terrorismus und organisierte Kriminalität oder geht es eher um Kontrolle und Begehrlichkeiten?

Am 6.1.2012 gab die dpa eine Kurzmeldung[1] über das Dreikönigstreffen der Münchner CSU heraus, die in diversen Medien veröffentlicht wurde. Laut dieser Meldung forderte Bundesinnenminister Dr. Hans-Peter Friedrich (CSU) Justizministerin Sabine Leutheusser-Schnarrenberger (FDP) erneut auf, den Widerstand gegen die Vorratsdatenspeicherung aufzugeben.

Nach Aussage Friedrichs wäre es unerträglich*, «wenn wir bewusst und gewollt unsere Ermittlungsbehörden blind machen»*. Technisch wäre es leicht zu realisieren, *«mit wem haben die Verbrecher im letzten halben Jahr telefoniert oder per E-Mail verkehrt. Dann hätten wir Namen und Fakten auf dem Tisch.»* Nach geltender Rechtslage sei jedoch *«alles gelöscht».*

Diese Aussagen bestätigen natürlich die Notwendigkeit, die Verkehrsdaten der Kommunikation zu speichern. Diese Daten können ohne Zweifel auch sehr effektiv gegen zweifelhafte Personengruppen zu Beweiszwecken eingesetzt werden. Aber ist die Vorratsdatenspeicherung wirklich allumfassend? Müssen die Bürger Angst haben, das private Nachrichten vom Staat mitgelesen werden?

Hier muss zuerst einmal zwischen den Begrifflichkeiten unterschieden werden: Telekommunikationsverkehrsdaten und Telekommunikationsinhalte.

Inhalte der Kommunikation, also die übermittelten Texte einer eMail beispielsweise, werden nicht gespeichert. Ausschließlich die Verkehrsdaten sollen über einem längeren Zeitraum gespeichert werden. Also die Information wann Manfred Mustermann von welchem Anschluss und mit welcher Benutzerkennung an Helga Mustermann eine eMail verfasst hat. Bei Telefon wäre das der bekannte Einzelverbindungsnachweis und der entsprechende Standort. In beiden Fällen muss auch die Anschrift des Anschlussinhabers gespeichert werden.

Die Speicherung der Daten wird dabei von den entsprechenden Anbietern von öffentlich zugänglichen Kommunikationsdiensten vorgenommen, die zur Speicherung verpflichtet werden sollen. Also sollen bekannte Anbieter wie Web.de, GMX, Freemail oder Yahoo diese Daten vorhalten.

Viele Bürger und Gegner sehen in dieser Speicherung der Daten einen Eingriff in das Persönlichkeitsrecht. Denn durch Standortspeicherung lassen sich z.B. Bewegungsprofile erstellen und bei der Analyse der eMail-Verkehrsdaten kann im Einzelfall auch die politische Ausrichtung nachgewiesen werden oder der Geschäftskontakt zu einer Liechtensteiner Bank. Liegen diese Daten erst einmal vor, so ist der Weg zur totalen Überwachung nicht mehr weit.

[1] http://www.focus.de/politik/deutschland/parteien-friedrich-dringt-auf-rasche-vorratsdatenspeicherung_aid_700162.html

Rechtfertigend für die Speicherung solcher Daten wären bahnbrechende Erfolge der Strafverfolgungsbehörden. Diese sind allerdings aktuell alles andere als vorzeigbar, weshalb man sich die Frage stellen kann, ob diese Speicherung der Verkehrsdaten nicht umgangen werden kann. Wäre dies möglich, wäre die Vorratsdatenspeicherung praktisch obsolet.

Eine Presseanfrage beim Bundesinnenministerium bezüglich der Aussagen Friedrichs bringt teilweise neue Erkenntnisse.

Auf die sinngemäße Frage, wie die Daten denn gespeichert werden sollen, antwortete ein Ministeriumssprecher:

"Die Europäische Richtlinie 2006/24/EG zur Vorratsdatenspeicherung verpflichtet die Mitgliedstaaten zur Einführung von Mindestspeicherfristen für Telekommunikationsverkehrsdaten, damit diese zur Verfolgung schwerer Straftaten den zuständigen Behörden zur Verfügung stehen. Danach müssen die Provider die jeweilige Benutzerkennung, die Anschrift des Anschlussinhabers sowie die Zeit der Verbindung und die Benutzerkennung, zu der eine Kommunikationsverbindung aufgebaut wurde für mindestens 6 Monate speichern.
Dies gilt ausweislich der Richtlinie auch für E-Mail-Provider. In Deutschland existierte eine entsprechende Regelung auch für Email-Provider bereits vom 01.01.2008 bis zum 02.03.2010 (§ 113a TKG). Die Weitergabe der Daten im konkreten Verdachtsfall an die zuständigen Behörden richtet sich nach den hierfür geltenden Vorschriften."

Im März 2010 kippte das Bundesverfassungsgericht ja die o.g. Regelung (BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 - 345)[2]

Zur Frage ob und wie denn bei Betrieb eines privaten eMail-Servers die Verkehrsdaten gespeichert werden können, antwortete ein Ministeriumssprecher:

"Die zitierten Vorschriften richten sich nur an Anbieter von öffentlich zugänglichen Kommunikationsdiensten."

Damit wäre ein erster Weg zur Umgehung der Datenspeicherung aufgezeigt. Betreiben kriminelle Elemente einen privaten Mailserver, der auch im Internet frei und kostenlos als Software heruntergeladen werden kann, so gibt es keine zuständige Stelle, die die Speicherung vornehmen könnte oder sollte.

Gegenüber dem Ministerium wurde auch die Möglichkeit angesprochen, dass eMail-Accounts außerhalb der EU bzw. auch sog. Einmal-Accounts verwendet werden können. Hier wurde zum einen auf die *"polizeiliche Zusammenarbeit bzw. internationale Rechtshilfeabkommen"* verwiesen und zum anderen genannt, dass für *"Einmal-Accounts dieselben rechtlichen Regelungen wie für dauerhaft genutzte Anschriften gelten"*. Explizit wurde betont, dass *"Name und Anschrift auch bei kostenlosen Angeboten [vom Service-Anbieter] vorzuhalten sind"*.

Diese Aussagen lassen prinzipiell verschiedene Möglichkeiten offen, der Vorratsdatenspeicherung zu entgehen:

1. **Benutzung von öffentlichen Websites** mit Chatfunktion oder Foren. Hier können in verschleierter Form Mitteilungen übertragen werden. Der Zugriff auf solche

[2] http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

Seiten kann oder sollte dann über öffentlich zugängliche, kostenlose WLANs erfolgen. Hierbei kann beispielsweise die IP-Adresse wie unter 2. genannt ausgetauscht werden: "Hi Fred, ruf mich doch mal kurz mobil an, 0171 - 91 20 78 20"

2. **Betreiben eines privaten Mail-Servers** z.B. auf dem eigenen Notebook. In der eMail-Adresse ist dabei keine namentliche Domain vorhanden sondern es wird beispielsweise eine Adresse in der Form Max@91.20.78.20 verwendet. Die notwendige aktuelle IP-Adresse wird dann vorher wie unter 1. genannt ausgetauscht, sofern diese nicht fest ist. Auch hier gibt es keine Instanz, die die Verkehrsdaten speichern könnte.

3. **Nutzung von kostenlosen eMail-Accounts**. Anbieter wie GMX, Yahoo oder Freemail bieten kostenlose eMail-Konten für Jedermann. Bei der Anmeldung müssen allerdings persönliche Daten inkl. Postadresse angegeben werden. In den AGBs der Anbieter wird genannt, das diese Angaben wahrheitsgemäß zu erfolgen haben. Bei Nichtbeachtung könne der Anbieter das Konto sperren. Allerdings kann man durchaus unterstellen, dass Terroristen nicht unbedingt die gesetzestreuesten Bürger sind. Hier greift zwar die Vorratsdatenspeicherung, aber wenn diese Konten nur zwei bis drei Mal benutzt werden ist die Wahrscheinlichkeit aufzufallen eher gering.

4. **Nutzung von Einmal-Accounts**. Es gibt durchaus eine Reihe deutscher Anbieter, die kurzlebige eMail-Adressen anbieten ohne persönliche Daten abzufragen. Websitebetreiber wie sofort-mail.de (der Menüpunkt 'Fragen & Antworten' sei hiermit wärmstens empfohlen!) oder safetypost.de bieten die Möglichkeit eine eMail-Adresse für eine extrem kurze Laufzeit - in der Regel wenige Minuten - zu nutzen. Hängt man an die eigene eMail die jeweils gültige Folgeadresse, so ist ohne Probleme eine flüssige Kommunikation möglich.

Fazit:

Bundesinnenminister Hans-Peter Friedrich mag auf dem Dreikönigstreffen Aussagen getroffen haben, die zwar kämpferisch und markig klingen; so richtig belastbar sind diese allerdings nicht.

Die Masse der Deutschen wird demnach von der Vorratsdatenspeicherung betroffen sein. Bei Menschen jeden Alters, ja sogar bei Kindern, wird ohne Anlass überwacht mit wem sie denn kommunizieren. Steht dann zu befürchten, dass man Hausbesuche zu erwarten hat, weil man die falschen Freunde hat, wie den Brieffreund aus Russland oder weil man bei der Steuererklärung geschummelt hat, dann wird das möglicherweise Beweis genug sein, dass diese Daten auch für kleinere Delikte herangezogen werden. Die Medienberichte der letzten Monate zeigen ziemlich deutlich, dass viele Behörden mit teilweise grenzwertigen Mittel zu Werke gehen (Trojaner, Mobilfunkortung, Rasterfahndung), selbst wenn es um Delikte geht, die eher nicht mit Terrorismus und organisierter Kriminalität zu vergleichen sind.

Ob potenzielle Straftäter so dumm sind von zu Hause mit vollständiger Adresse und immer gleicher eMail-Adresse über Attentate und Bombenbau zu philosophieren, sei dahingestellt. Prinzipiell kann jeder Kriminelle heute schon aus dem Fernsehen die Grundregeln lernen, wie man Fehler vermeidet.

Warum brauchen wir dann die Vorratsdatenspeicherung?

Für weitere Fragen und Informationen stehen wir Ihnen gerne jederzeit zur Verfügung:

Proteus Solutions GbR
Björn-Lars Kuhn

Meisenweg 5
78549 Spaichingen

Tel: (0 74 24) 94 00 13 – 70
oder kostenlos unter:
0800 – 50 50 60 55
Fax: (0 74 24) 94 00 13 - 77

Email: BLK@proteus-solutions.de
Web: www.proteus-solutions.de

Proteus Solutions GbR
Björn-Lars Kuhn